

675.29.13

19 November 2004

**Arbeitspapier zu Lehrplänen zur Internetsicherheit unter Berücksichtigung nationaler,  
kultureller und rechtlicher (einschließlich datenschutzrechtlicher) Anforderungen**

*- angenommen bei der 36. Sitzung am 18./19. November 2004 in Berlin -*

**Sicherheit von Informationssystemen**

In der frühen Entwicklungszeit der Automation war die Sicherheit von Informationssystemen vor allem mit bescheidenen Stand-alone-Systemen in geschlossenen Netzwerken befasst und war entsprechend in ihrer Reichweite begrenzt auf die Übernahme relativ einfacher Regeln für die physische, hard- und softwaremäßige Sicherheit.

Später haben die starke Zunahme von immer leistungsfähigeren Personalcomputern, die Verbreitung neuer Informations- und Kommunikationstechnologien, der umfassende Gebrauch des Internet und die zunehmende Abhängigkeit menschlicher Aktivitäten von einem ordnungsgemäßen Funktionieren der Informationssysteme die Situation komplexer gemacht.

Heute kann die Sicherheit von Informationssystemen nicht mehr begrenzt werden auf Gegenmaßnahmen gegen Symptome angesichts technischer Sicherheitsbedrohungen, sondern es ist nötig, elementare Änderungen von Verhaltensmustern von allen Beteiligten einzuführen, um den eindringlichen Bedrohungen zu begegnen, denen menschliche Werte und Menschenrechte durch die Sicherheit im Internet ausgesetzt sind.

Dieser neue globale und systematische Zugang zur Informationssicherheit ist unterstrichen und vorangetrieben worden durch die OECD, deren Veröffentlichung „Guidelines for the Security of Information Systems and Networks“ die Notwendigkeit anerkennt, eine echte „Sicherheitskultur“ zu entwickeln.

Secretariat  
Berliner Beauftragter für  
Datenschutz und Informationsfreiheit  
An der Urania 4- 10  
D-10787 Berlin  
Phone +49 / 30 / 13889 0  
Fax: +49 / 30 / 215 5050

E-Mail:  
[IWGDPT@datenschutz-berlin.de](mailto:IWGDPT@datenschutz-berlin.de)  
  
Internet:  
<http://www.datenschutz-berlin.de>

The Working Group has been initiated  
by Data Protection Commissioners  
from different countries in order  
to improve privacy and data protection  
in telecommunications and media

## **Sicherheit von Informationssystemen versus Datenschutz**

Um ihre jeweiligen Aufgaben zu erfüllen, müssen heute alle Organisationen, gleich ob es öffentliche oder private Stellen sind, eine zunehmende Menge von Daten einschließlich immer mehr personenbezogenen Daten in ihren Informationssystemen erheben, verarbeiten und speichern.

Das Recht auf informationelle Selbstbestimmung ist ein Grundrecht und ein wirksamer Datenschutz kann nicht erreicht werden ohne angemessene Sicherheit. Das ist bereits 1980 durch die „OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data“ anerkannt worden. Da Sicherheit zwingend erforderlich ist, um Persönlichkeitsrechte zu schützen, verlangt der spezifische gesetzliche Schutz personenbezogener Daten im Vergleich zu anderen Daten und deren Sicherheit oft einen völlig verschiedenen Zugang. Die fundamentalen Datenschutzprinzipien wie das Recht auf Vergessen, das Recht auf Zugang, die Begrenzung der Erhebung und Verarbeitung sowie das Verhältnismäßigkeitsprinzip sind bedauerlicherweise keine grundsätzlichen Prinzipien, die von Sicherheitsexperten notwendigerweise anerkannt werden.

## **Informationssicherheitsexperten**

Heute hat sich die Sicherheit von Informationssystemen nicht nur mit den technischen Risiken der verschiedenen Computerplattformen, Netzwerke, Protokolle oder anderen Bestandteilen von Informationssystemen zu befassen, sondern hat ebenso andere Risiken in Betracht zu ziehen, wie sie mit der Organisation des Unternehmens und ihren Verfahrensweisen zusammenhängen, solche, die sich auf Personaldaten beziehen oder solche, die mit den bestehenden rechtlichen Beschränkungen zusammenhängen wie etwa dem Datenschutz oder dem Urheberrecht.

Diese multidisziplinäre Wahrnehmung von Risiken ist in der Welt von Informationssicherheitsexperten nicht die Regel. Zu oft wird die Sicherheit von Informationssystemen noch als eine Angelegenheit für Computer- oder Technikexperten betrachtet und darüber hinaus nur begrenzt auf prophylaktische technische Maßnahmen, mit der Folge komplexer Sicherheitssysteme, die in einer Zunahme technischer Kontrollen von zweifelhafter Bedeutung resultieren, die den Datenschutz durchaus beeinträchtigen können.

Selbst wenn der Bedarf an hochausgebildeten Sicherheitsexperten umfassend anerkannt ist, gibt es wenige konkrete strukturierte Initiativen, um die bestehenden Erwartungen zu erfüllen. Oft ist der Begriff eines Informationssicherheitsberaters weder eingeführt, definiert noch durch gesetzliche Regelungen umschrieben. Der Zugang zu diesem Beruf ist einem Zertifizierungsprozess überlassen, der durch private Institutionen organisiert wird.

## **Empfehlungen**

Angesichts dieser Situation empfiehlt die Arbeitsgruppe angesichts der erstrangigen Rolle, die die Sicherheit von Informationssystemen und der Datenschutz beim ordnungsgemäßen Funktionieren von Organisationen spielen, dass:

- das Konzept eines Informationssystemssicherheitsberaters unterstützt wird, der dem CISO-Konzept (Corporate Information Security Officer) entspricht, das in verschiedenen internationalen Normen und Veröffentlichungen beschrieben wird, und das alle notwendigen Datenschutzaspekte umfasst.
- Angesichts der Verantwortungen, die mit der Ausübung einer solchen Funktion verbunden sind, besteht unzweifelhaft der Bedarf höherer Professionalität. Sehr oft erfordern diese Funktionen einen Hochschulabschluss. Demgemäß sollte eine akademische oder berufsbildende Qualifikation für Informationssystemssicherheitsberater eingeführt werden, die eine Ausbildung gewährleistet, die die nationalen rechtlichen und kulturellen Traditionen berücksichtigt und die so neutral und unabhängig von wirtschaftlichen Interessen ausgestaltet ist wie irgend möglich. Zertifiziert werden sollten mit der

Qualifikation alle notwendigen technischen Kenntnisse über Sicherheit, die einschlägigen Managementfähigkeiten, Wissen darüber, wie Sicherheit am besten organisiert werden kann, Kenntnis fundamentaler Datenschutzregelungen und schließlich alle relevanten rechtlichen Kenntnisse, die Sicherheitsberater in die Lage versetzen, ihre Rolle innerhalb der Organisation korrekt auszufüllen.